UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,117	06/30/2000	Kelan C. Silvester	042390.P8691	1041

7590 03/30/2004

Walter T Kim
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	4

DATE MAILED: 03/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/608,117	SILVESTER, KELAN C.	
	Examin r	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondenc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3, 4, and 7-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones et al. (U.S. Patent No. 5,623,637).

Regarding claim 1, Jones et al. teaches a method comprising:

- Providing a partition on a storage device of a computer system (col. 5, lines 32-34),
    - Wherein said partition is normally invisible to an operating system of the computer system unless the partition is unlocked (col. 5, lines 54-59);
- Unlocking the partition in response to an unlock request received from a software task having knowledge about a proper handshake to unlock the partition (col. 5, lines 59-67),
    - Wherein the partition is visible to the operating system when it is unlocked (col. 6, lines 1-4); and
- Preventing an access to the partition when the partition is unlocked unless the access is requested by a software having knowledge about a proper handshake

for accessing the partition (col. 8, lines 4-34, the particular method of combining passwords, random numbers, and an unlock code has to be known by the requesting software in order for the unlocking to be performed properly).

Jones et al. does not specifically teach that the partition is normally invisible unless unlocked, but rather that the partition is inaccessible by any device driver software until the partition is unlocked.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to make certain partitions inaccessible to any device driver software unless unlocked by an authorization signal, as taught by Jones et al. It would have been obvious to make certain partitions inaccessible to any device driver software unless unlocked by an authorization signal, because this prevents the secured partition from exchanging information with the host (col. 4, lines 47-50).

Regarding claim 3, Jones et al. as modified teaches wherein the unlocking of the partition is initiated by establishing a proper unlock handshake between the software task and an IDE controller for controlling the storage device (col. 8, lines 9-34 & fig. 2).

Jones et al. does not teach an IDE controller for controlling the storage device. However, Jones et al. does teach PCMCIA interface control terminals and an internal control bus (col. 3, lines 64-67).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to use a PCMCIA interface control terminal and an internal control bus, as taught by Jones et al. It would have been obvious to use a PCMCIA interface control terminal and an internal control bus because the interface provides a way to exchange control signals from the secure storage area to the host computer.

Regarding claim 4, Jones et al. as modified teaches wherein the software task requests a master token from the IDE controller when the computer system is first turned on and the unlock handshake between the software task and the IDE controller is established by passing the master token back to the IDE controller as a parameter (col. 7, lines 52-58 and col. 8, lines 9-34).

Regarding claim 7, Jones et al. as modified teaches wherein the software receives a usage token from an IDE controller when the partition is unlocked and the access handshake between the software and the IDE controller is established by passing the usage token back to the IDE controller as a parameter (the Examiner takes Official Notice that this action is required in public-key cryptography. IDE controller sends a public key to the software, the software encrypts its request with the public key of the IDE controller, and the IDE controller decrypts the request with its private key).

Regarding claim 8, Jones et al. as modified teaches further comprising locking the partition in response to a lock request received from a software having knowledge about a proper handshake for locking the partition (col. 7, lines 21-31).

Regarding claim 9, Jones et al. as modified teaches further comprising providing a standard partition on the storage device (col. 7, lines 32-35), wherein said standard partition is always visible to the operating system and generally accessible to other software (col. 7, lines 32-35).

Regarding claim 10, Jones et al. teaches a machine-readable medium that provides instructions, which when executed by a set of processors, causes said set of processors to perform operations comprising:

- Receiving an open request from a software to access a secure-private partition on a hard drive of a computer system (col. 5, lines 54-59);
- Validating the open request received from the software (col. 5, lines 59-64);
- Requesting unlocking of the secure-private partition in response to the validation of the open request received from the software (col. 5, lines 64-67);
- Unlocking the secure-private partition in response to the unlocking request, wherein the secure-private partition is visible to an operating system when the secure-private partition is unlocked (col. 5, lines 59-67 and col. 6, lines 1-4); and
- Preventing an access to the secure-private partition when the secure-private partition is unlocked unless the access is requested by a software having

knowledge about a proper access handshake for accessing the secure-private partition (col. 8, lines 4-34, the particular method of combining passwords, random numbers, and an unlock code has to be known by the requesting software in order for the unlocking to be performed properly).

Jones et al. does not specifically teach the partition is on a hard drive. However, Jones et al. teaches the partition on a storage device (col. 5, lines 32-34).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to partition a storage device, as taught by Jones et al. It would have been obvious to partition a storage device, because the partitioned storage device allows some of the partitions to be accessible by software and devices, and other partitions to be inaccessible by software and devices (col. 7, lines 32-35). This allows a secure storage area.

Regarding claim 11, Jones et al. as modified teaches wherein the operations further comprise requesting locking of the secure-private partition in response to a close request received from the software (col. 7, lines 21-31).

Regarding claim 12, Jones et al. as modified teaches wherein the requesting of the unlocking of the secure partition further comprises:

- Requesting a master token from an IDE controller when the computer system is turned on (col. 7, lines 52-58);
- Storing the master token in a secure storage location (col. 8, lines 6-9);
- Retrieving the master token from the secure storage location when an access to a secure-private partition is needed (col. 8, lines 9-34); and
- Passing the master token as a parameter to the IDE controller (col. 8, lines 20-24).

Regarding claim 13, Jones et al. as modified teaches wherein the operations further comprise requesting an access to the secure-private partition in response to an access request received from the software (col. 6, lines 1-4).

Regarding claim 14, Jones et al. as modified teaches wherein the requesting of the access to the secure partition further comprises:

- Receiving a usage token (fig. 2, ref. num 303 and col. 8, lines 9-13); and
- Passing the usage token to the IDE controller to gain an access to the secure partition (fig. 2, ref. num 307 and col. 8, lines 9-19).

Regarding claim 15, Jones et al. as modified teaches wherein the request from the software to access the secure-private partition is received by a privacy gatekeeper which prescreens the request to determine if the software has an authorization to access the secure-private partition (col. 7, lines 52-59 describes authorizing the request

as soon as the card is inserted, or at first turning on the computer. This is the prescreening, if the authorization fails, the computer system knows the device is not authorized for future transactions, and vice versa.).

Regarding claim 16, Jones et al. teaches a system comprising:

- A storage device having a storage controller (fig. 1, ref. num 100),
    - Said storage device having at least one secure-private partition (fig. 1, ref. num 150),
    - Wherein said secure-private partition is selectively in one of locked and unlocked modes (col. 7, lines 21 and 36),
    - Wherein said secure-private partition is invisible to an operating system when it is locked and the secure-private partition is visible to the operating system when it is unlocked (col. 5, lines 54-59 and col. 6, lines 1-4);
- An IDE controller operatively coupled to the storage controller (col. 3, lines 64-67); and
- A security/privacy software task operatively coupled to the IDE controller (fig. 1, ref. num 220),
    - Wherein said IDE controller initiates an unlock request to unlock the secure-private partition in response to a valid unlock handshake established between the IDE controller and the security/privacy software task (col. 5, lines 59-67) and

- Said IDE controller initiates a lock request to lock the secure-private partition in response to a valid lock handshake established between the IDE controller and the security/privacy software task (col. 7, lines 21-31),
- Wherein the IDE controller generates and returns a usage token to the requesting software once the secure-private partition is unlocked, wherein the access handshake is established between the IDE controller and the requesting software when the IDE controller validates the usage token passed back by the requesting software (col. 8, lines 4-34, the particular method of combining passwords, random numbers, and an unlock code has to be known by the requesting software in order for the unlocking to be performed properly).

Jones et al. does not specifically teach the partition is invisible when locked, nor does he teach an IDE controller operatively coupled to the storage controller. However, Jones et al. does teach the partition is inaccessible by any device driver software when the partition is locked (col. 5, lines 54-59) and a PCMCIA interface control terminals and an internal control bus couple to the storage controller (col. 3, lines 64-67).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to make certain partitions inaccessible to any device driver software unless unlocked by an authorization signal and to use a PCMCIA interface control terminal and an internal control bus, as taught by Jones et al. It would have

been obvious to make certain partitions inaccessible to any device driver software unless unlocked by an authorization signal and to use a PCMCIA interface control terminal and an internal control bus, because this prevents the secured partition from exchanging information with the host (col. 4, lines 47-50) and the interface provides a way to exchange control signals from the secure storage are to the host computer.

Regarding claim 17, Jones et al. as modified teaches wherein the security/privacy software task requests a master token from the IDE controller when the system is turned on and sends the master token to the IDE controller as a parameter when making a request to the IDE controller to unlock the secure-private partition (col. 7, lines 52-58 and col. 8, lines 9-34).

Regarding claim 18, Jones et al. as modified teaches further comprising a requesting software and a privacy gatekeeper which acts as a gatekeeper to the security/privacy software task (fig. 1, ref. num 178), wherein when the requesting software makes a request to access the secure-private partition (col. 5, lines 59-67), the privacy gatekeeper prescreens the request to determine if the requesting software has an authorization to access the secure-private partition (col. 7, lines 52-59 describes authorizing the request as soon as the card is inserted, or at first turning on the computer.).

Regarding claim 19, Jones et al. as modified teaches wherein the IDE controller allows an access to said at least one secure-private partition only when a valid access handshake is established between the requesting software and the IDE controller (col. 8, lines 9-34 & fig. 2).

Claims 2 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones et al. (U.S.P.N. '637) in view of Hamasaka et al. (U.S. Patent No. 5,485,439).

Regarding claim 2, Jones et al. teaches all the limitations of claim 1 above. However, Jones et al. does not teach wherein the storage device is a hard disk drive having a disk controller.

Hamasaka et al. teaches wherein the storage device is a hard disk drive having a disk controller (fig. 8, ref. num 8200).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a hard disk having a disk controller, as taught by Hamasaka et al., with the method of Jones et al. It would have been obvious to combine a hard disk having a disk controller, as taught by Hamasaka et al., with the method of because a hard disk is a large volume storage device contained in computer systems that store software programs that can utilize the large hard disk storage.

Regarding claim 5, Jones et al. as modified by Hamasaka et al. teaches wherein the software task requests a master token from the disk controller when the computer system is first turned on (see col. 7, lines 52-58 of Jones et al.), said master token is used by the software task to initiate the proper handshake to unlock the partition (see col. 8, lines 4-34 of Jones et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Brandon Hoffman

BH
3/24/04

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100